

## CLAIMS

What is claimed is:

SUB A17

1. A method comprising:
  - 2 authenticating a user of a platform during a Basic Input/Output System (BIOS)
  - 3 boot process;
  - 4 releasing a first keying material from a token communicatively coupled to the
  - 5 platform in response to authenticating the user;
  - 6 combining the first keying material with a second keying material internally
  - 7 stored within the platform in order to produce a combination key; and
  - 8 using the combination key to decrypt a second BIOS area to recover a second
  - 9 segment of BIOS code.
2. The method of claim 1 further comprising:
  - 2 continuing the BIOS boot process.
3. The method of claim 1, wherein prior to authenticating the user, the method comprises:
  - 3 loading a BIOS code including a first BIOS area and a second BIOS area, the
  - 4 first BIOS area being an encrypted first segment of the BIOS code and the second
  - 5 BIOS area being an encrypted second segment of the BIOS code.
4. The method of claim 3, wherein after loading of the BIOS code, the method further comprises:
  - 3 decrypting the first BIOS area to recover the first segment of the BIOS code.
5. The method of claim 1 further comprising:
  - 2 unbinding keying material associated with a non-volatile storage device to
  - 3 access contents stored within the non-volatile storage device.
6. The method of claim 1 wherein the combination key is a value formed
  - 2 by performing an exclusive OR operation on both the first keying material and the
  - 3 second keying material.

1           7.     The method of claim 1, wherein authentication of the user is performed  
2 through biometrics.

1           8.     The method of claim 1, wherein the second keying material is stored  
2 within internal memory of a trusted platform module.

1           9.     The method of claim 1, wherein the second keying material is stored  
2 within a section of access-controlled system memory of the platform.

1           10.    The method of claim 1, wherein prior to authenticating the user, the  
2 method comprises:  
3           loading a BIOS code including a first BIOS area being a first segment of the  
4 BIOS code encrypted using a selected keying material; and  
5           loading an integrity metric including a hash value of an identification  
6 information of the platform.

1           11.    The method of claim 1, wherein the identification information includes a  
2 serial number of an integrated circuit device employed within the platform.

1           12.    An integrated circuit device comprising:  
2           a boot block memory unit; and  
3           a trusted platform module communicatively coupled to the boot block memory  
4 unit, the trusted platform module to produce a combination key by combining a first  
5 incoming keying material with a second keying material internally stored within the  
6 integrated circuit and to decrypt a second BIOS area to recover a second segment of  
7 BIOS code.

1           13.    The integrated circuit device of claim 12, wherein the boot block  
2 memory unit to load a BIOS code including a first BIOS area and a second BIOS area,  
3 the first BIOS area being an encrypted first segment of the BIOS code and the second  
4 BIOS area being an encrypted second segment of the BIOS code.

1           14.    The integrated circuit device of claim 13, wherein the trusted platform  
2 module to decrypt the first BIOS area to recover a first segment of the BIOS code.

1       ~~15.~~ A platform comprising:  
2           an input/output control hub (ICH);  
3           a non-volatile memory unit coupled to the ICH, the non-volatile memory unit  
4 including a BIOS code including a first BIOS area and a second BIOS area, the first  
5 BIOS area being an encrypted first segment of the BIOS code and the second BIOS  
6 area being an encrypted second segment of the BIOS code; and  
7           a trusted platform module coupled to the ICH, the trusted platform module to  
8 produce a combination key by combining a first incoming keying material with a  
9 second keying material internally stored within the platform and to decrypt the second  
10 BIOS area to recover the second segment of BIOS code.

1           16. The platform of claim 15, wherein the trusted platform module to further  
2 decrypt the first BIOS area to recover the first segment of the BIOS code in an non-  
3 encrypted format.

1           17. The platform of claim 15 further comprising a hard disk drive coupled to  
2 the ICH.

1           18. The platform of claim 17, wherein the trusted platform module to further  
2 unbind keying material associated with the hard disk drive to access contents stored  
3 within the hard disk drive.

1       ~~19.~~ A program loaded into readable memory for execution by a trusted  
2 platform module of a platform, the program comprising:  
3           code to decrypt a first Basic Input/Output System (BIOS) area to recover a first  
4 segment of BIOS code;  
5           code to produce a combination key by combining a first incoming keying  
6 material with a second keying material internally stored within the trusted platform  
7 module; and  
8           code to decrypt a second BIOS area to recover a second segment of the BIOS  
9 code.

1           20.    The program of claim 19, wherein the first BIOS area is the first  
2   segment of the BIOS code encrypted with a keying material and the second BIOS area  
3   is the second segment of the BIOS code encrypted with the combination key.

1           21.    The program of claim 19 further comprising:  
2           code to unbind keying material associated with a non-volatile storage device for  
3   accessing contents stored within the non-volatile storage device.